PacketViper Delivers Command-Level Protection for Semiconductor Fab Equipment

SECS/GEM command control governs recipe and remote-command traffic inline, agentless, on one appliance, providing fabs compensating control aligned to SEMI E187

PITTSBURGH, PA, UNITED STATES, July 10, 2026 /EINPresswire.com/ -- PacketViper today announced SECS/GEM command control, extending its OT protocol command control platform to the equipment that runs semiconductor manufacturing. The capability reads SECS/GEM traffic down to the individual command, understands what that command is trying to do to a tool, and lets a fab decide which commands are allowed, from which sources, at what rate. It is generally available now.

> “Fabs run some of the most valuable and least forgiving processes on earth, and the most dangerous thing an attacker
> can do is send a command the tool was never designed to question.”
>
> *Francesco Trama*

Semiconductor fab equipment communicates with the host and manufacturing execution system using SECS/GEM over HSMS. Like most industrial protocols, SECS/GEM was designed for reliable communication on a trusted network, not for authenticating the command. If a message reaches a tool and speaks the protocol, the tool obeys. That means a process program, better known as a recipe, a remote command that starts or stops a tool, or an equipment constant change is honored the same way whether it came from the authorized host or from a system that does not belong on the line. A single unauthorized or tampered recipe can scrap a wafer lot and damage tooling. Much of the installed base of fab equipment cannot meet modern cybersecurity requirements on its own.

PacketViper closes that gap at the command, on the wire, in real time. It decodes each SECS/GEM message to the level of the actual operation, separates routine data collection from the small set of commands that can change what a tool does, and governs that dangerous set per tool. Fabs decide which sources may download a recipe, which may issue a remote command, and which may change an equipment constant. Everything else is flagged or blocked, scoped to that one tool.

The capability runs inline as a transparent, agentless bridge in front of the equipment. There is no IP to route to, no software to install on a tool, and no change to the equipment or the host. It starts in observation mode so it never disrupts a running process, then narrows to surgical enforcement on the operations that carry risk. The capture path is fail open, so protection never

becomes the reason a tool stops.

Because every governed command is recorded with its source, target, operation, and outcome, the audit trail is a byproduct of running the system. PacketViper serves as an enforced compensating control aligned to the SEMI E187 and E188 cybersecurity requirements, protecting equipment that cannot meet those requirements natively and generating the evidence a fab needs to demonstrate control.

SECS/GEM command control is one layer of PacketViper's patented Automated Moving Target Defense. On the same single appliance, PacketViper delivers deception, sensors, asset discovery, and command-level control across the broader industrial protocol landscape. Static defenses get mapped over time. A moving, layered defense does not.

"Fabs run some of the most valuable and least forgiving processes on earth, and the most dangerous thing an attacker can do is send a command the tool was never designed to question," said Francesco Trama, CEO and Founder, PacketViper. "We put that command under governance. The authorized host still does its job, and an unauthorized recipe or remote command is stopped before it reaches the tool, on one appliance, without touching the equipment."
SECS/GEM command control is available now as part of the PacketViper platform. Existing customers can enable it per tool in observation mode and narrow to enforcement on their own schedule.

About PacketViper
PacketViper is a U.S. owned Automated Moving Target Defense company. Its single appliance delivers command-level protocol control, deception, sensors, and asset discovery across information technology and operational technology environments, protecting critical infrastructure and the legacy systems that cannot run agents or tolerate disruption. PacketViper starts open and narrows in, so security never becomes the reason a process stops.

Tim Jencka
PacketViper
+1 412-212-6348
email us here
